KING & SPALDING, LLP

1180 Peachtree Street NE
Atlanta, Georgia 30309-3521
Telephone: 404/572-4600
Facsimile: 404/572-5100
www.kslaw.com

FAX TRANSMITTAL SHEET

February 20, 2007

TO:	**Mail Stop Appeal Brief-Patents** Commissioner for Patents U.S. Patent Application No. 09/844,448	**Company:**	U.S. Patent and Trademark Office
	Fax #: 571-273-8300	**City/State:**	Alexandria, VA 22313
FROM:	Kerry L. Broome 3443	**Our Ref. #:**	05456.105005

NUMBER OF PAGES (including transmittal sheet): 39

If transmission problems occur or you are not the intended recipient, please call 404.572.4647 immediately. Thank you.

Notes/Comments:

Documents Submitted Via Facsimile:

Applicant:	Gregory Neil Houston et al.
Serial No.:	09/844,448
Filed:	April 27, 2001
For:	System and Method for Managing Security Events on a Network
Papers Faxed:	Transmittal for Appeal Brief and duplicate (2-pgs.); Credit Card Payment Form (PTO-2038) (1-pg.); and Appeal Brief (35-pgs.)

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: **Gregory Neil Houston et al.**	Atty Docket: **05456.105005**
Application No.: **09/844,448**	Art Unit: **2135**
Filing Date: **April 27, 2001**	Examiner: **Linh Son**
Title: **System and Method for Managing Security Events on a Network**	Confirmation No.: **9082**

TRANSMITTAL FOR APPEAL BRIEF

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicants hereby appeal to the Board of Patent Appeals and Interferences from the last decision of the Examiner dated November 17, 2006.

Please charge $500.00 for the fee for filing a brief in support of the appeal required under 37 C.F.R. § 41.20(b)(2) to the credit card payment form (PTO-2038) which is attached hereto.

The Commissioner is authorized to charge any additional fee required for this Notice of Appeal, or to credit any overpayment, to Deposit Account No. 11-0980. A duplicate of this paper is enclosed.

Respectfully submitted,

Kerry L. Broome

Kerry L. Broome
Attorney for Applicants
Reg. No. 54,004

KING & SPALDING LLP
1180 Peachtree Street, N.E., 34th Floor
Atlanta, Georgia 30309-3521
(404) 572-4600

I hereby certify that this correspondence is being facsimile transmitted to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450, Facsimile No. (571) 273-8300, on February 20, 2007.

Kerry L Broome

Kerry L. Broome, Reg. No. 54,004

RECEIVED
CENTRAL FAX CENTER

FEB 2 0 2007

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: **Gregory Neil Houston et al.**	Atty Docket: **05456.105005**
Application No.: **09/844,448**	Art Unit: **2135**
Filing Date: **April 27, 2001**	Examiner: **Linh Son**
Title: **System and Method for Managing Security Events on a Network**	Confirmation No.: **9082**

TRANSMITTAL FOR APPEAL BRIEF

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicants hereby appeal to the Board of Patent Appeals and Interferences from the last decision of the Examiner dated November 17, 2006.

Please charge $500.00 for the fee for filing a brief in support of the appeal required under 37 C.F.R. § 41.20(b)(2) to the credit card payment form (PTO-2038) which is attached hereto.

The Commissioner is authorized to charge any additional fee required for this Notice of Appeal, or to credit any overpayment, to Deposit Account No. 11-0980. A duplicate of this paper is enclosed.

Respectfully submitted,

Kerry L. Broome

Kerry L. Broome
Attorney for Applicants
Reg. No. 54,004

KING & SPALDING LLP
1180 Peachtree Street, N.E., 34th Floor
Atlanta, Georgia 30309-3521
(404) 572-4600

I hereby certify that this correspondence is being facsimile transmitted to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450, Facsimile No. (571) 273-8300, on February 20, 2007.

Kerry L. Broome

Kerry L. Broome, Reg. No. 54,004

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: **Gregory Neil Houston et al.**	Atty Docket: **05456.105005**
Application No.: **09/844,448**	Art Unit: **2135**
Filing Date: **April 27, 2001**	Examiner: **Linh Son**
Title: **System and Method for Managing Security Events on a Network**	Confirmation No.: **9082**

APPEAL BRIEF

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Sir:

In support of the notice of appeal mailed on February 15, 2007 in the above referenced application, Appellants hereby submit this brief under 37 C.F.R. § 1.191 to appeal the Examiner's rejection of this application as reported in the Official Action mailed on November 17, 2006.

I hereby certify that this correspondence is being facsimile transmitted to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450, Facsimile No. (571) 273-8300, on February 20, 2007.

Kerry L. Broome

Kerry L. Broome, Reg. No. 54 004

Table of Contents

Real Party in Interest

The real party in interest is IBM Internet Security Services, formerly operating as Internet Security Systems, Inc., the assignee of record.

Related Appeals and Interferences

None.

Status of Claims

Claims 1-59 stand finally rejected and are on appeal. Appeal is taken from the rejection of all pending claims.

Status of Amendments

No additional amendments have been filed subsequent to the final rejection mailed on November 17, 2006.

Summary of Claimed Subject Matter

In general, the invention disclosed by the present application defines a new system and process that facilitates the management of security events on a distributed computer network. More specifically, the security management system can collect, store, filter, and analyze security event data in order to facilitate managing the security for a relatively large computing network. A user can create customized scopes of varying criteria for filtering the data so that only the desired information is provided to a user. Scopes can also be customized to analyze security event data for responding to or anticipating a security event. By storing the security event data, the invention supports the retrieval of additional information about each event if needed. Improving the ability to manage security event data from a network further supports the capacity to respond to a security event when necessary.

Independent Claim 1 is directed to a computer-implemented method for gathering security event data and rendering result data in a manageable format in a computer network. The computer implemented method comprises the following steps, along with the associated portions of the specification that support these steps: (1) generating security event data comprising a plurality of alerts with a plurality of security devices at a first location in response to detecting a security event in a distributed computing environment (page 7, lines 24-27; page 11, lines 7-16); (2) providing one or more variables operable for analyzing and filtering the security event data (page 8, lines 17-23), the variables comprising at least one of a location of a security event, a source of security event, a destination address of the security event, a security event type, a priority of a security event, and an identification of a system that detected a security event (page 9, lines 27-30); (3) creating scope criteria by selecting one or more of the variables operable for analyzing and filtering the security event data (page 8, lines 17-23; page 9, line 25 to page 10, line 10); (4) collecting the security event data generated by the plurality of security devices located at the first location (page 7, lines 10-11; page 7, lines 24-27; page 11, lines 7-16); (5) storing the collected security event data at a second location (page 7, lines 27-29); (6) analyzing and filtering the collected security event data with the scope criteria to produce result data (page 8, lines 25-28; page 11, line 17 to page 12, line 5); (7) transmitting the result data to one or more clients (page 12, lines 13-25); and (8) displaying the result data comprising filtered alerts based on the scope criteria (page 12, lines 6-12; page 14, lines 8-20).

Independent Claim 16 is directed to a method for managing security event data collected from a plurality of security devices in a distributed computing environment. The method comprises the following steps, along with the associated portions of the specification that support these steps: (1) generating security event data comprising a plurality of alerts with the plurality of security devices at a first location in response to detecting a security event in a distributed computing environment (page 7, lines 24-27; page 11, lines 7-16); (2) providing one or more variables operable for analyzing and filtering the security event data (page 8, lines 17-23), the variables comprising at least one of a location of a security event, a source of security event, a destination address of the security event, a security event type, a priority of a security event, and an identification of a system that detected a security event (page 9, lines 27-30); (3) creating scope criteria by selecting one or more of the variables operable for analyzing and filtering the security event data (page 8, lines 17-23; page 9, line 25 to page 10, line 10); (4) collecting security event data at a second location (page 7, lines 10-11; page 7, lines 24-27; page 11, lines 7-16); (5) applying the scope criteria to the security event data at a third location to produce result data (page 8, lines 25-28; page 11, line 17 to page 12, line 5); (6) transmitting the result data to one or more clients (page 12, lines 13-25); and (7) displaying the result data comprising filtered alerts based on the scope criteria (page 12, lines 6-12; page 14, lines 8-20).

Independent Claim 27 is directed to a computer-implemented system for managing security event data collected from a plurality of security devices. The system comprises the following elements, along with the associated portions of the specification that support these elements: (1) a plurality of security devices operable for generating security event data comprising a plurality of alerts that are generated in response to detecting a security event in a distributed computing environment (page 7, lines 6-7; page 7, lines 24-27); (2) an event manager coupled to the security devices (page 7, lines 24-25), the event manager operable for collecting the security event data from the security devices (page 7, lines 10-11; page 7, lines 24-27; page 11, lines 7-16) and analyzing and filtering the security event data with scope criteria comprising one or more definable variables operable for analyzing and filtering the security event data (page 8, lines 17-28; page 11, line 17 to page 12, line 5), the variables comprising at least one of a location of a security event, a source of security event, a destination address of the security event, a security event type, a priority of a security event, and an identification of a system that detected a security event (page 9, lines 27-30), and applying the scope criteria to the security

event data to produce result data (page 8, lines 25-28; page 11, line 17 to page 12, line 5); and (3) one or more clients coupled to the event manager (page 8, lines 12-19) operable to perform an action in response to receiving analyzed security event data from the event manager (page 12, lines 13-25) and displaying the result data comprising filtered alerts based on the scope criteria (page 12, lines 6-12; page 14, lines 8-20).

Independent Claim 34 is directed to a computer-implemented method for gathering security event data and rendering result data in a manageable format. The method comprises the following steps, along with the associated portions of the specification that support these steps: (1) generating security event data comprising a plurality of alerts with a plurality of security devices at a first location in response to detecting a security event in a distributed computing environment (page 7, lines 24-27; page 11, lines 7-16); (2) providing one or more variables operable for analyzing and filtering the security event data (page 8, lines 17-23), the variables comprising at least one of a location of a security event, a source of security event, a destination address of the security event, a security event type, a priority of a security event, and an identification of a system that detected a security event (page 9, lines 27-30); (3) creating scope criteria by selecting one or more of the variables operable for analyzing and filtering the security event data (page 8, lines 17-23; page 9, line 25 to page 10, line 10); (4) collecting the security event data at a second location (page 7, lines 10-11; page 7, lines 24-27; page 11, lines 7-16); (5) analyzing and filtering the collected security event data with the scope criteria at a third location to produce result data (page 8, lines 25-28; page 11, line 17 to page 12, line 5); (6) transmitting the result data to one or more clients (page 12, lines 13-25); and (7) rendering the result data, in a manageable format for the one or more clients (page 12, lines 6-12; page 14, lines 8-20).

Independent Claim 49 is directed to a method for managing security event data collected from a plurality of security devices in a distributed computing environment. The method comprises the following steps, along with the associated portions of the specification that support these steps: (1) generating security event data with a plurality of security devices in response to detecting a security event in a distributed computing environment, the security event data comprising a plurality of alerts (page 7, lines 24-27; page 11, lines 7-16); (2) transferring the security event data for storage in a database (page 7, lines 27-29); (3) applying a scope criteria comprising one or more definable variables to the security event data for analyzing and filtering the security event data to produce a result (page 8, lines 17-23), the variables comprising at least

one of a location of a security event, a source of security event, a destination address of the security event, a security event type, a priority of a security event, and an identification of a system that detected a security event (page 8, lines 25-28; page 9, lines 27-30; page 11, line 17 to page 12, line 5); (4) accessing the result with one or more clients coupled to an application server (page 12, lines 1-5; page 12, lines 13-25); and (5) displaying the result data comprising filtered alerts based on the scope criteria (page 12, lines 6-12; page 14, lines 8-20).

Grounds of Rejection to be Reviewed on Appeal

The following issues are presented on appeal:

(1) Whether, under 35 U.S.C. § 102(e), Claims 27-29 and 31-32 are anticipated by U.S. Patent No. 6,088,804 (Hill).

(2) Whether Claims 1-26, 30, and 33-59 are obvious under 35 U.S.C. § 103(a) over U.S. Patent No. 6,088,804 (Hill) and/or U.S. Patent No. 6,775,657 (Baker).

Argument

Rejection of claims as obvious over 35 U.S.C. § 102(e)

The Legal Standard for 35 U.S.C. § 102(e)

An invention must be new at the time of discovery by an original inventor to be patentable. See Chisum, PATENTS, Vol. 1, § 3.01, p. 3-3. Section 101 of Title 35, U.S.C. requires that a patentable invention must be "new." The meaning of "new" is defined by specific conditions set forth in Section 102. Specifically, § 102(b), provides:

> A person shall be entitled to a patent unless . . . (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for the purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Under Section 102(e), the issue is strict novelty of the invention (i.e., anticipation). Thus, prior art references are examined to determine whether any one reference discloses the entire claimed invention within its "four corners." To anticipate the claimed invention, each and every element of the claimed invention must be disclosed in the reference. As mentioned, the standard for lack of novelty (i.e., anticipation) is one of strict identity. To anticipate a claim for a patent, a single prior source must contain all its essential elements. See Hybritech Inc. v. Monoclonal Antibodies, Inc., 802 F.2d 1367, 1379 (Fed. Cir. 1986) ("It is axiomatic that for prior art to anticipate under § 102 it has to meet every element of the claimed invention, and that such a determination is one of fact.

A traditional way of looking at the law of anticipation invalidity is as follows: "That which infringes, if later, would anticipate if earlier." Knapp v. Morss, 14 S.Ct. 81, 84 (1893). "That which will infringe, if later, will anticipate, if earlier. Thus a claim fails to meet the novelty requirement if it covers or reads on a product or process found in a single source in the prior art." Lewmar Marine, Inc. v. Barient, Inc., 827 F.2d 744, 747 (Fed. Cir. 1987) "The standard for lack of novelty, that is, for 'anticipation,' is one of strict identity. To anticipate a

claim for a patent, a single prior source must contain all its essential elements." See Chisum, § 3.02[1], p. 3-14. "The law of anticipation does not require that the reference 'teach' what the subject patent teaches. Assuming that a reference is properly 'prior art,' it is only necessary that the claims under attack, as construed by the court, 'read on' something disclosed in the reference, i.e., all limitations of the claim are found in the reference, or 'fully met' by it." Kalman v. Kimberly-Clark Corp., 713 F.2d 760, 771 (Fed. Cir. 1983).

Analysis

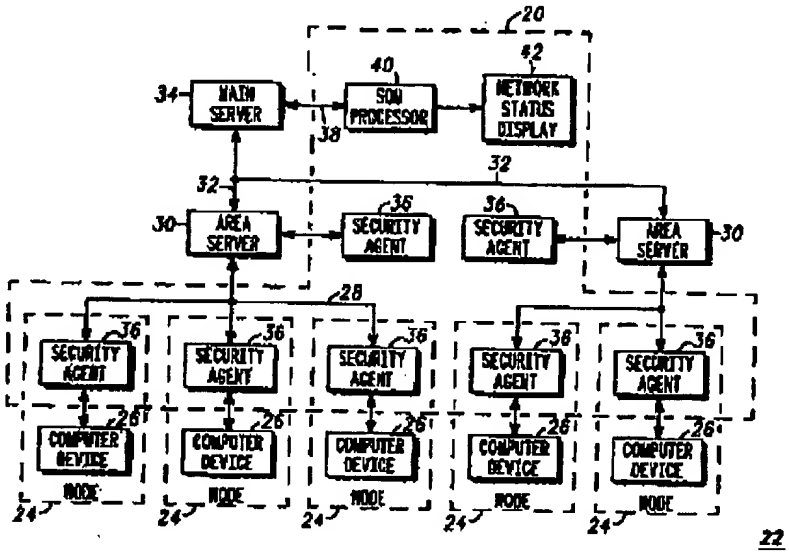
The Hill reference disclosed by Examiner for the rejection of independent Claim 27 under 35 U.S.C. § 102(e) fails to disclose recitations that are present in the independent claim. Specifically, as rejected by the Examiner in the Final Office Action mailed on 11/17/06, the Hill reference fails to disclose or suggest the claimed feature of "the event manager operable for collecting the security event data from the security devices and analyzing and filtering the security event data with scope criteria comprising one or more definable variables operable for analyzing and filtering the security event data."

Independent Claim 27

On pages 4-5 of the Final Office Action mailed on 11/18/06, the Examiner directs the Applicants' attention to Column 5 line 39 to Column 6 line 20 of the Hill reference, to teach the claimed feature of "the event manager operable for...analyzing and filtering the security event data with scope criteria comprising one or more definable variables operable for analyzing and filtering the security event data." However, this particular recitation from Hill merely provides how Hill uses simulated attacks to respond to actual security attacks. As described below, the Hill reference fails to teach for analyzing and filtering the security event data with scope criteria.

In general, the Hill reference describes a dynamic network security system (20) that responds to a security attack on a computer network (22) having a multiplicity of computer nodes (24). The security system (20) includes a plurality of security agents (36) that concurrently detect occurrences of security events on associated computer nodes (24). A processor (40) processes the security events that are received from the security agents (36) to form an attack signature of the attack. A network status display (42) displays multi-dimensional attack status

information representing the attack in a two dimensional image to indicate the overall nature and severity of the attack. See Figure 1 of the Hill system reproduced below.



As shown in Figure 3 of the Hill reference below, a database (48) maintains the simulated attack information for a plurality of simulated attacks (52). Each of the simulated attacks (52) is a prediction of an attack type that may occur on network (22). Simulated attacks (52) are generated by an operator and stored in database (48). Each simulated attack (52) contains a training signature (53) that is defined by a plurality of security events (50) of at least one security event type (56). Security events (50) are presented in database (48) in a column (58) as a percentage of security events per event type.

In addition to security event types (56) and percentage of security events (50) per event type in column (58), training signatures (53) include location identifiers (60). Location identifiers (60) identify the nodes (24) in network (22) where security events may take place. Location identifiers (60) are important for ascertaining an attack severity (61) for each of simulated attacks (52). Attack severity (61) is a level of security breach that one of simulated attacks (52) could cause computer network (22).

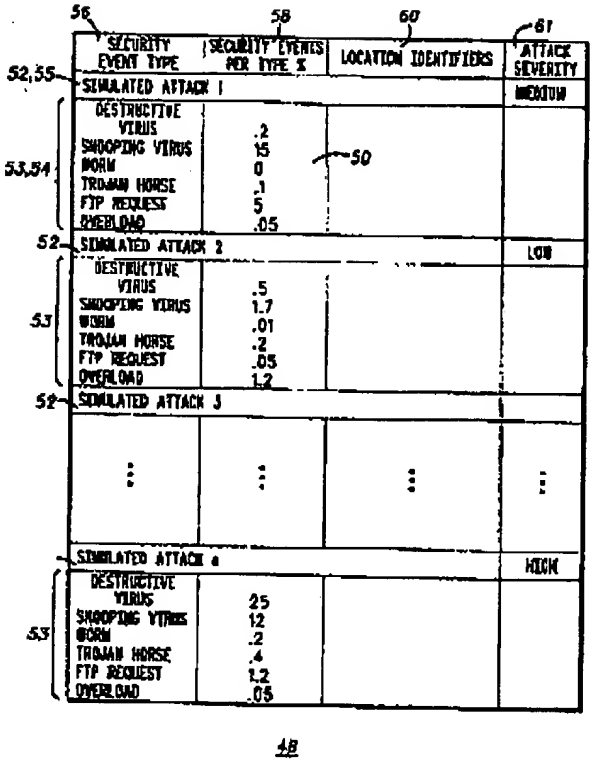


FIG. 3

As shown in Figure 7 of the Hill reference below, a network status display (42) displays multi-dimensional attack status information in a two dimensional image to indicate the overall nature and severity of an attack. The network status display (42) presents a display map (66) and an attack status information list (108) showing security event type (56) and location identifiers (60) for an example attack (92). The network status display (42) also presents an attack signature log (110) which provides current and historical perspective on a given attack record at various sample times. The attack signatures in log (110) are the text equivalent of the two dimensional image as highlighted in display map (66). In addition, the network status display (42) includes an attack mitigation list (112) which is a catalogue of actions that a network manager may take in order to mitigate the example attack (92).

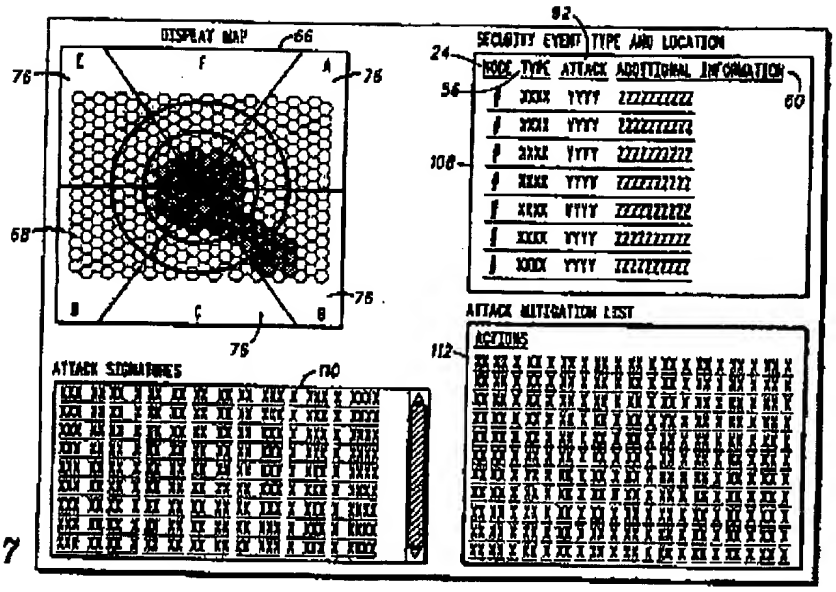


FIG. 7

In summary, the Hill reference teaches generating simulated attacks that may occur on the network. These simulated attacks comprise training signatures that define what types of security events are present in each attack. In response to the simulated attacks, the system in the Hill reference can subsequently be trained to detect and respond to actual security attacks by monitoring and analyzing the network traffic data. Subsequently, in response to an actual security attack, the system in the Hill reference can respond with an action that corresponds to a simulated attack that is stored in the database. Furthermore, in response to an actual security attack, the Hill reference can present a display map containing attack information.

Therefore, the Hill reference fails to teach the claimed feature of an event manager that is operable for analyzing and filtering the security event data with scope criteria comprising one or more definable variables operable for analyzing and filtering the security event data. The Hill reference merely teaches displaying (1) multi-dimensional attack status information showing security event type and location identifiers for an example attack; (2) an attack signature log which provides current and historical perspective on a given attack record at various sample times; and (3) an attack mitigation list which is a catalogue of actions that a network manager may take in order to mitigate the example attack. The Hill reference fails to teach that this information can be analyzed or filtered with scope criteria.

Simply displaying attack status information is not the same as "analyzing and filtering the security event data with scope criteria comprising one or more definable variables operable for

analyzing and filtering the security event data." The Hill reference fails to teach that attack status information can be analyzed or filtered with scope criteria. Furthermore, Column 5 line 39 to Column 6 line 20 of the Hill reference, as cited by the Examiner to reject this feature is completely silent on analyzing and filtering the security event data with scope criteria. Applicants submit that the invention of independent Claim 27 is not anticipated by the reference of record.

Dependent Claims 28-33

The Applicants respectfully submit that the above-identified dependent claims are allowable because Independent Claim 27 from which they depend is patentable over the cited prior art reference. The Applicants also respectfully submit that the recitations of these dependent claims are of patentable significance.

In view of the foregoing, the Applicants respectfully request that the Examiner withdraw the pending rejections of dependent Claims 28-33.

Rejection of claims as obvious over 35 U.S.C. § 103(a)

The Legal Standard for 35 U.S.C. § 103(a)

The U.S. patent and Trademark Office has the burden under 35 U.S.C. § 103 to establish a *prima facie* case of obviousness. *In re Warner et al.*, 379 F.2d 1011, 154 U.S.P.Q. 173, 177 (C.C.P.A. 1967), *In re Fine*, 837 F.2d 1071, 1074, 5 U.S.P.Q.2d 1596, 1598-99 (Fed. Cir. 1988). To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicants' disclosure. *In re Vaeck, 947 F.2d 488, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991).* The references cited by the Examiner do not meet all three criteria.

The prior art must provide one of ordinary skill in the art with the motivation to make the proposed modification needed to arrive at the claimed invention. *In re Geiger*, 815 F.2d 686, 2 U.S.P.Q.2d 1276 (Fed. Cir. 1987); *in re Lalu and Foulletier*, 747 F.2d 703, 705, 223 U.S.P.Q. 1257, 1258 (Fed. Cir. 1984). Claims for an invention are not *prima facie* obvious if the primary references do not suggest all elements of the claimed invention and the prior art does not suggest the modifications that would bring the primary references into conformity with the application claims. *In re Fritch*, 23 U.S.P.Q.2d, 1780 (Fed. Cir. 1992). *In re Laskowski*, 871 F.2d 115 (Fed. Cir. 1989). This is not possible when the claimed invention achieves more than what any or all of the prior art reference allegedly suggest, expressly or by reasonable implication.

The Court of Appeals for the Federal Circuit warned that "the best defense against the subtle but powerful attraction of a hindsight-based obviousness analysis is rigorous application of the requirement for showing of the describing or motivation to combine prior art references." *In re Dembiczak*, 175 F.3d 994 at 999 (Fed. Cir. 1999). The Examiner has not provided such a showing.

It is clear that to establish a rejection under 35 U.S.C. § 103 the cited references must (1) recite each element of the claims, (2) provide one of skill in the art with the motivation to combine the cited reference as applications have done and (3) provide one of ordinary skill in the art with a reasonable expectation of success. The references cited by the Examiner clearly do not meet all three criteria and the current rejection of the claims-in-issue lack proper support.

Analysis

The Hill and Baker references disclosed by Examiner for the rejection of independent Claims 1, 16, 34, and 49 under 35 U.S.C. § 103(a) fail to disclose multiple recitations that are present in the independent claims. Specifically, as rejected by the Examiner in the Final Office Action mailed on 11/17/06, the Hill and Baker references fail to disclose or suggest the claimed features of: (1) "providing one or more variables operable for analyzing and filtering the security event data, the variables comprising at least one of a location of a security event, a source of security event, a destination address of the security event, a security event type, a priority of a security event, and an identification of a system that detected a security event;" (2) "creating scope criteria by selecting one or more of the variables operable for analyzing and filtering the

security event data;" and (3) "analyzing and filtering the collected security event data with the scope criteria to produce result data."

As noted, independent Claims 1, 16, 34, and 49 are subject to the same ground of rejection as allegedly being obvious under 35 U.S.C. § 103(a) in view of the Hill and Baker references. Therefore, Applicants will group all of the independent claims on appeal and argue these particular claim recitations with respect to independent Claim 1 only.

Furthermore, Applicants respectfully note that the arguments made with regards to the rejections of independent Claims 1, 16, 34, and 49 as allegedly being obvious under 35 U.S.C. § 103(a) in view of the Hill and Baker references are similar to the arguments made with regards to the rejection of independent Claim 27 as allegedly being anticipated under 35 U.S.C. § 102(e) in view of the Hill reference. Therefore, references will be made to the arguments above to avoid repetition of previously stated arguments.

Independent Claims 1, 16, 34, and 49

> *Hill and Baker do not disclose or suggest the claimed features of "providing one or more variables operable for analyzing and filtering the security event data, the variables comprising at least one of a location of a security event, a source of security event, a destination address of the security event, a security event type, a priority of a security event, and an identification of a system that detected a security event" and "creating scope criteria by selecting one or more of the variables operable for analyzing and filtering the security event data"*

On pages 7-9 of the Final Office Action mailed on 11/18/06, the Examiner directs the Applicants' attention to Column 5, line 39 to Column 6, line 20 to teach the claimed features of "providing one or more variables operable for analyzing and filtering the security event data, the variables comprising at least one of a location of a security event, a source of security event, a destination address of the security event, a security event type, a priority of a security event, and an identification of a system that detected a security event" and "creating scope criteria by selecting one or more of the variables operable for analyzing and filtering the security event data." However, this particular recitation from Hill merely provides how Hill uses simulated attacks to respond to actual security attacks. As described previously and applicable here, the Hill reference fails to teach providing one or more variables operable for analyzing and filtering the security event data with scope criteria.

As stated above with respect to the rejection under § 102(e), the Hill reference fails to teach the claimed features of "providing one or more variables operable for analyzing and filtering the security event data" and "creating scope criteria by selecting one or more of the variables operable for analyzing and filtering the security event data." The Hill reference merely teaches displaying (1) multi-dimensional attack status information showing security event type and location identifiers for an example attack; (2) an attack signature log which provides current and historical perspective on a given attack record at various sample times; and (3) an attack mitigation list which is a catalogue of actions that a network manager may take in order to mitigate the example attack. The Hill reference fails to teach that this information can be analyzed or filtered with scope criteria.

Once again, simply displaying attack status information is not the same as "analyzing and filtering the security event data with scope criteria comprising one or more definable variables operable for analyzing and filtering the security event data." The Hill reference fails to teach that attack status information can be analyzed or filtered with scope criteria. Furthermore, Column 5 line 39 to Column 6 line 20 of the Hill reference, as cited by the Examiner to reject these features is completely silent on analyzing and filtering the security event data with scope criteria.

Hill and Baker do not disclose or suggest the claimed feature of "analyzing and filtering the collected security event data with the scope criteria to produce result data"

On page 9 of the Final Office Action mailed on 11/17/06, the Examiner directs the Applicants' attention to Column 8, lines 25-46 of the Hill reference to teach the claimed feature of "analyzing and filtering the collected security event data with the scope criteria to produce result data." Once again, to reiterate the arguments described above, the Hill reference fails to teach that the security event data can be analyzed and filtered with scope criteria.

Furthermore, Column 8, lines 25-46 of the Hill reference, as cited by the Examiner to reject this feature is completely silent on analyzing and filtering the security event data with scope criteria. This particular section of the Hill reference merely discloses how the system of Hill selects which training signature most closely matches the attack signature by comparing a vector representative of an attack signature to each of the training signatures. The purpose of

this step is to determine which training signature is used to respond to an attack signature. This recitation does not teach analyzing and filtering collected security event data with the scope criteria to produce result data.

The remarks presented above with respect to independent Claim 1 are equally applicable to independent Claims 16, 34, and 49. Applicants submit that independent Claims 1, 16, 34, and 49 are not obvious over the references of record. Therefore, Applicants respectfully request that the Examiner withdraw the pending rejection of independent Claims 1, 16, 34, and 49.

Dependent Claims 2-15, 17-26, 35-48, and 50-59

The Applicants respectfully submit that the above-identified dependent claims are allowable because the independent claims, namely Claims 1, 16, 34, and 49, from which they depend are patentable over the cited prior art references. The Applicants also respectfully submit that the recitations of these dependent claims are of patentable significance.

In view of the foregoing, the Applicants respectfully request that the Examiner withdraw the pending rejections of dependent Claims 2-15, 17-26, 35-48, and 50-59.

Conclusion

In view of the arguments presented herein, Applicants respectfully request that the final rejection in this matter be vacated, and that this application be returned to the examiner with instructions to enter a notice of allowance.

Respectfully submitted,

Kerry L. Broome

Kerry L. Broome
Reg. No. 54,004

KING & SPALDING LLP
1180 Peachtree Street
34th Floor
Atlanta, GA 30309
(404) 572-4600 (Telephone)
(404) 572-5134 (Facsimile)

APPENDIX 1

CLAIMS APPENDIX

1. (Previously Presented) A computer-implemented method for gathering security event data and rendering result data in a manageable format comprising the steps of:

generating security event data comprising a plurality of alerts with a plurality of security devices at a first location in response to detecting a security event in a distributed computing environment;

providing one or more variables operable for analyzing and filtering the security event data, the variables comprising at least one of a location of a security event, a source of security event, a destination address of the security event, a security event type, a priority of a security event, and an identification of a system that detected a security event;

creating scope criteria by selecting one or more of the variables operable for analyzing and filtering the security event data;

collecting the security event data generated by the plurality of security devices located at the first location;

storing the collected security event data at a second location;

analyzing and filtering the collected security event data with the scope criteria to produce result data;

transmitting the result data to one or more clients; and

displaying the result data comprising filtered alerts based on the scope criteria.

2. (Original) The method of Claim 1, further comprising storing one or more of the scope criteria and the result data.

3. (Original) The method of Claim 1, wherein the first location is a distributed computing environment and the second location is a database server.

4. (Original) The method of Claim 1, wherein collecting the security event data comprises

generating security event data from a sensor;
sending the security event data from the sensor to a collector; and
converting the event data to a common format.

5. (Original) The method of Claim 1, wherein the analyzing is performed at an application server to which the plurality of clients are coupled.

6. (Original) The method of Claim 1, further comprising searching the stored security event data for additional information identifying a security event.

7. (Original) The method of Claim 1, further comprising:
polling a database server for current stored security event data;
analyzing the current stored security event data to produce current result data; and
rendering the current result data.

8. (Original) The method of Claim 1, further comprising polling for messages containing information about scope criteria, security event data, or result data.

9. (Original) The method of Claim 1, further comprising pushing messages to a client wherein the messages contain information about scope criteria, security event data, or result data.

10. (Original) The method of Claim 1, wherein the step of rendering result data comprises presenting the result data in a chart format.

11. (Original) The method of Claim 1, wherein in response to analyzing the collected security event data, an action is executed.

12. (Original) The method of Claim 11, wherein the action is clearing security event data from storage.

13. (Original) The method of Claim 11, wherein the action is creating an incident from result data for preparing a response.

14. (Original) The method of Claim 1, wherein the step of collecting security event data further comprises converting the data to a uniform format.

15. (Original) A computer-readable medium having computer-executable instructions for performing the steps recited in Claim 1.

[The Remainder of this page has been intentionally left blank.]

16. (Previously Presented) A method for managing security event data collected from a plurality of security devices in a distributed computing environment comprising the steps of:

generating security event data comprising a plurality of alerts with the plurality of security devices at a first location in response to detecting a security event in a distributed computing environment;

providing one or more variables operable for analyzing and filtering the security event data, the variables comprising at least one of a location of a security event, a source of security event, a destination address of the security event, a security event type, a priority of a security event, and an identification of a system that detected a security event;

creating scope criteria by selecting one or more of the variables operable for analyzing and filtering the security event data;

collecting security event data at a second location;

applying the scope criteria to the security event data at a third location to produce result data;

transmitting the result data to one or more clients; and

displaying the result data comprising filtered alerts based on the scope criteria.

17. (Original) The method of Claim 16, further comprising rendering the result in a rendering for output to a client.

18. (Original) The method of Claim 16, wherein the first location is a distributed computing environment.

19. (Original) The method of Claim 16, wherein the second location is a database server.

20. (Original) The method of Claim 16, wherein the third location is an application server coupled to the plurality of clients.

21. (Original) The method of Claim 16, further comprising storing one or more of the scope criteria, the security event data, and the result in a database.

22. (Original) The method of Claim 16, further comprising executing an action at the server in response to producing the result.

23. (Original) The method of Claim 22, wherein the action is clearing stored security event data.

24. (Original) The method of Claim 22, wherein the action is creating an incident from a result.

25. (Original) The method of Claim 16, further comprising applying additional scope criteria to a plurality of results.

26. (Original) A computer-readable medium having computer-executable instructions for performing the steps recited in Claim 16.

[The Remainder of this page has been intentionally left blank.]

27. (Previously Presented) A computer-implemented system for managing security event data collected from a plurality of security devices comprising:

a plurality of security devices operable for generating security event data comprising a plurality of alerts that are generated in response to detecting a security event in a distributed computing environment;

an event manager coupled to the security devices, the event manager operable for collecting the security event data from the security devices and analyzing and filtering the security event data with scope criteria comprising one or more definable variables operable for analyzing and filtering the security event data, the variables comprising at least one of a location of a security event, a source of security event, a destination address of the security event, a security event type, a priority of a security event, and an identification of a system that detected a security event, and applying the scope criteria to the security event data to produce result data; and

one or more clients coupled to the event manager operable to perform an action in response to receiving analyzed security event data from the event manager and displaying the result data comprising filtered alerts based on the scope criteria.

28. (Previously Presented) The system of Claim 27, wherein the event manager comprises a database server operable for storing the collected security event data and the analyzed security event data.

29. (Original) The system of Claim 27, wherein the event manager comprises an application server operable for creating an incident from the security event data for preparing a response.

30. (Original) The system of Claim 27, wherein the security devices are coupled to a distributed computing network.

31. (Original) The system of Claim 27, wherein multiple clients operable for receiving analyzed security data are coupled to the event manager.

32. (Original) The method of Claim 27, wherein the action performed by the client is rendering a chart containing analyzed security event data.

33. (Original) The method of Claim 1, further comprising the step of rendering the result data in a manageable format for the plurality of clients.

[The Remainder of this page has been intentionally left blank.]

34. (Previously Presented) A computer-implemented method for gathering security event data and rendering result data in a manageable format comprising the steps of:

generating security event data comprising a plurality of alerts with a plurality of security devices at a first location in response to detecting a security event in a distributed computing environment;

providing one or more variables operable for analyzing and filtering the security event data, the variables comprising at least one of a location of a security event, a source of security event, a destination address of the security event, a security event type, a priority of a security event, and an identification of a system that detected a security event;

creating scope criteria by selecting one or more of the variables operable for analyzing and filtering the security event data;

collecting the security event data at a second location;

analyzing and filtering the collected security event data with the scope criteria at a third location to produce result data,

transmitting the result data to one or more clients; and

rendering the result data, in a manageable format for the one or more clients.

35. (Original) The method of Claim 34, further comprising storing one or more of the scope criteria, the security event data, and the result data.

36. (Original) The method of Claim 34, wherein the first location is a distributed computing environment, the second location is a database server, and the third location is an application server to which the plurality of clients are coupled.

37. (Original) The method of Claim 34, further comprising editing the scope criteria.

38. (Original) The method of Claim 34, further comprising converting the collected security event data to a common format.

39. (Original) The method of Claim 35, further comprising searching the stored security event data for additional information identifying a security event.

40. (Original) The method of Claim 35, further comprising:
polling a database server for current stored security event data;
analyzing the current stored security event data to produce current result data; and
rendering the current result data.

41. (Original) The method of Claim 34, further comprising polling for messages containing information about scope criteria, security event data, or result data.

42. (Original) The method of Claim 34, further comprising pushing messages to a client wherein the messages contain information about scope criteria, security event data, or result data.

43. (Original) The method of Claim 34, wherein the step of rendering the result data comprises presenting the result data in a chart format.

44. (Original) The method of Claim 34, wherein in response to analyzing the collected security event data, an action is executed.

45. (Original) The method of Claim 44, wherein the action is clearing security event data from storage.

46. (Original) The method of Claim 44, wherein the action is creating an incident from result data for preparing a response.

47. (Original) The method of Claim 34, wherein the step of collecting security event data further comprises converting the data to a uniform format.

48. (Original) A computer-readable medium having computer-executable instructions for performing the steps recited in Claim 34.

49. (Currently Amended) A method for managing security event data collected from a plurality of security devices in a distributed computing environment comprising the steps of:

generating security event data with a plurality of security devices in response to detecting a security event in a distributed computing environment, the security event data comprising a plurality of alerts;

transferring the security event data for storage in a database;

applying a scope criteria comprising one or more definable variables to the security event data for analyzing and filtering the security event data to produce a result, the variables comprising at least one of a location of a security event, a source of security event, a destination address of the security event, a security event type, a priority of a security event, and an identification of a system that detected a security event;

accessing the result with one or more clients coupled to an application server; and

displaying the result data comprising filtered alerts based on the scope criteria.

50. (Original) The method of Claim 49, further comprising rendering the result in a rendering for output to the clients.

51. (Original) The method of Claim 49, further comprising the step of creating the scope criteria for filtering the security event data.

52. (Original) The method of Claim 49, further comprising the step of editing the scope criteria.

53. (Original) The method of Claim 49, further comprising converting the security event data to a uniform format.

54. (Original) The method of Claim 49, further comprising storing one or more of the scope criteria, the security event data, and the result in a database.

55. (Original) The method of Claim 49, wherein in response to producing a result, an action is executed.

56. (Original) The method of Claim 55, wherein the action is clearing stored security event data.

57. (Original) The method of Claim 55, wherein the action is creating an incident from a result.

58. (Original) The method of Claim 49, further comprising applying additional scope criteria to a plurality of results.

59. (Original) A computer-readable medium having computer-executable instructions for performing the steps recited in Claim 49.

[The Remainder of this page has been intentionally left blank.]

APPENDIX 2

EVIDENCE APPENDIX

None.

APPENDIX 3

RELATED PROCEEDINGS APPENDIX

None.